

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, et al.

Plaintiffs

vs.

BRAD RAFFENSPERGER, et al.

Defendants

)

)

)

)

) Case No.

) 1:17-CV-2989-AT

)

)

)

)

VIDEOTAPED VIDEOCONFERENCE DEPOSITION OF
JUAN GILBERT, Ph.D.
Friday, October 29, 2021
Volume I

Reported by:

CARLA SOARES

CSR No. 5908

Job No. 4871592

Pages 1 - 289

INDEX

WITNESS

JUAN GILBERT, Ph.D.

EXAMINATION

Volume I

BY MR. CROSS

9

EXHIBITS

NUMBER

DESCRIPTION

PAGE

Exhibit 1

10

Declaration of Dr. Juan Gilbert

Exhibit 2

41

Document entitled "Georgia Voter
Verification Study"

Exhibit 3

56

United States Patent,
No. US 11.036,442 B2

Exhibit 4

141

Article entitled "Why computer
scientists prefer paper ballots"

EXHIBITS

| NUMBER | DESCRIPTION | PAGE |
|------------------------------------|--|------|
| Exhibit 5 | Document labeled "Exhibit A" | 179 |
| Exhibit 6 | E-mail string, top e-mail to Scott Tucker from Michael Barnes, dated 1-15-20 | 209 |
| Exhibit 7 | Twitter page | 260 |
| Exhibit 8 | Letter to Juan E. Gilbert, Ph.D. from Bryan P. Tyson, dated 11-8-19 | 270 |
| Exhibit 9 | Trial transcript, dated 3-24-09 | 274 |
| (Exhibits attached to transcript.) | | |

1 JUAN GILBERT, Ph.D.,
2 having been administered an oath, was examined and
3 testified as follows:

4 MR. CROSS: Before we begin the
5 questioning, is everybody on -- does everybody here
6 have access to the Exhibit Share or is it only the
7 lawyers and the witness?

8 VERITEXT CONCIERGE: Everybody should have
9 access.

10 MR. CROSS: Okay. We need -- can we go
11 off the record? I didn't realize that.

12 THE VIDEO OPERATOR: Okay. Going off the
13 record at 10:07.

14 (Recess, 10:07 a.m. - 10:09 a.m.)

15 THE VIDEO OPERATOR: Back on the record at
16 10:09.

17 EXAMINATION

18 BY MR. CROSS:

19 Q Good morning, Dr. Gilbert.

20 A Good morning.

21 Q Can you hear me okay?

22 A Yes, I can.

23 Q Is there any reason why you feel you
24 cannot testify truthfully and completely today?

25 A No.

1 said, "incomplete report."

2 Q You said you read what was given to you.
3 I just wanted to confirm that, to your
4 understanding, what was given to you was
5 Dr. Halderman's complete July 1 report; is that
6 right?

7 A Yes.

8 Q Did I understand correctly, you reviewed
9 that report carefully before responding to it,
10 right?

11 A Yes.

12 Q But nowhere in your July 16 declaration do
13 you indicate that you've conducted any examination
14 of any election equipment used in Georgia; is that
15 right?

16 A Correct. I have not examined any
17 equipment.

18 Q You did not think that was relevant to
19 respond to Dr. Halderman's analysis, examining that
20 equipment?

21 A In my response, no.

22 Q Why not?

23 A I only responded to things that I could
24 respond to without having examined the equipment
25 using the expertise that I have in the area.

1 Q Why didn't you examine the equipment
2 yourself so that you could respond to his precise
3 findings where he examined the equipment?

4 A I was not provided the equipment.

5 Q Did you ask for it?

6 A No.

7 Q Why not?

8 A I believe I mentioned this in the
9 declaration or previous declarations. I was not
10 aware that that was an option for me to have
11 equipment given the nature of past cases where this
12 equipment was never given to experts. So it's
13 just -- it's something that never crossed my mind.

14 Q That's an exchange that you and I had in
15 the September hearing where I asked you in September
16 of last year why you did not look at the equipment.
17 But you knew as of July this year when you prepared
18 your declaration that Dr. Halderman had access to
19 election equipment from Fulton County; right, sir?

20 A I believe so, looking at that declaration,
21 yes.

22 Q Even though you knew Dr. Halderman had
23 access, even though you were reviewing and
24 responding to his report regarding that access, you
25 did not think it was relevant to ask for access to

1 the equipment yourself?

2 A No.

3 MR. MILLER: Objection to form. Asked and
4 answered.

5 BY MR. CROSS:

6 Q You think it's appropriate for an expert
7 who's opining on the security and reliability of an
8 election system not to actually examine that system
9 for himself?

10 A Yes.

11 Q You don't actually -- in your declaration
12 from July of this year, you don't actually offer any
13 disagreement with any of Dr. Halderman's findings
14 based on his analysis of that equipment; correct,
15 sir?

16 A Can you elaborate on what finding in
17 particular, or specific findings?

18 Q Any of them.

19 A I need to know exactly which findings.

20 Q Okay. Well, direct me to your -- a
21 portion of your July 16 declaration where you
22 disagree with any of his findings in his July 1
23 report.

24 A I don't understand -- you said disagree
25 with any of his findings.

1 Dr. Gilbert, you keep saying it did not occur to you
2 to examine the election equipment even though you
3 knew Dr. Halderman was examining it.

4 Can you explain that to me? Why would it
5 not occur to you to look at election equipment where
6 you are tasked with responding to the expert who has
7 himself examined that equipment?

8 MR. MILLER: Objection. Asked and
9 answered.

10 THE WITNESS: Because I didn't see it as a
11 necessity. I wasn't going to get the equipment and
12 break the equipment or replicate his hacks.

13 BY MR. CROSS:

14 Q But couldn't -- there's no other analysis
15 you could have done with the equipment to respond to
16 his report?

17 A The analysis that I have done I feel is
18 sufficient to respond to his report.

19 Q But you've done no analysis of any
20 election equipment used in the State of Georgia; is
21 that correct, sir?

22 MR. MILLER: Objection.

23 THE WITNESS: I have not had access to any
24 equipment in the State of Georgia.

25 ///

1 Georgia should take before proceeding with the
2 current election equipment in light of
3 Dr. Halderman's findings?

4 A I can't think of anything at this time.
5 I'd have to go back and review, again, his report
6 and do a point-by-point measure.

7 And I would also say that the RLA is --
8 again, getting at the QR code, the RLA would also be
9 a measure to identify differences between QR codes
10 and the human-readable portion of the text.

11 Q One of the measures you said the state
12 should take is reminding voters to verify their
13 ballots before they're scanned or tabulated, right?

14 A Yes.

15 Q Do you understand Georgia already requires
16 that?

17 A I may have read that. It wasn't at the
18 top of my mind.

19 Q Given that Georgia already requires that,
20 why would you expect that to have a meaningful
21 impact on the security and reliability of this
22 election system?

23 A Reminding voters did show some improvement
24 on voters verifying their ballots.

25 Q In fact, the Rice study and the Michigan

1 this year for which you are the inventor; right,
2 sir?

3 A Yes, this appears to be the patent.

4 Q Have you seen this patent before?

5 A This appears to be what we submitted, yes.

6 Q If you turn to the page -- it looks like
7 it's -- if you go past the figures, so after
8 Figure 6, you'll get to where it starts to describe
9 the patent, and it has "Transparent Interactive
10 Printing Interface."

11 Do you see that?

12 A Yes.

13 Q And this concerns the new BMD prototype
14 that we've been discussing today that you developed,
15 right?

16 A Yes.

17 Q Do you see under "Background"?

18 A Yes.

19 Q Do you see what's written here in this
20 patent that you helped prepare, and for which you're
21 identified as the inventor, it reads,
22 "Ballot-marking devices (BMDs) such as electronic
23 ballot markers (EBMs) electronically-assisted ballot
24 markers, in voting machines are often
25 nontransparent, hackable, and overly complex."

1 That's written here; correct, sir?

2 A Yes, it is.

3 Q It also goes on, "Such conventional
4 devices often result in a trade-off between
5 consistency and transparency," right?

6 A Yes.

7 Q And at the end it reads, "It is typically
8 difficult or impossible to fully examine and trace
9 the process and result of entering selections for a
10 ballot using conventional BMDs and EMDs."

11 Do you see that?

12 A Yes, I do.

13 Q In preparing the patent for which you're
14 identified as an inventor, were you careful to be
15 accurate and truthful in the information that you
16 included there?

17 A I was careful to be truthful in the
18 information and as accurate as possible using
19 language that I've seen in other places about BMDs.

20 These are allegations against BMDs. And I
21 would say I don't necessarily agree with all the
22 allegations, but these are common allegations
23 against BMDs. So I'm stating what is the common
24 allegation against BMDs. And that's why it's in
25 background, to say these are the common allegations

1 against BMDs.

2 Q Dr. Gilbert, nowhere here does it say that
3 these are allegations that you do not believe to be
4 true; right, sir?

5 A Right. In a patent submission, I don't
6 think I would say that I don't agree with these or I
7 don't believe these things. I wouldn't say that in
8 a patent application.

9 What I'm doing is stating what is commonly
10 said or communicated in the -- in a community around
11 BMD allegations.

12 These allegations that I am setting forth
13 are -- even right as we're here now -- are the bases
14 for these allegations. So these are, I would argue,
15 common -- common allegations that are said.

16 Q Dr. Gilbert, do you understand you're
17 under oath today?

18 A Yes, I am under oath, and I would say --

19 Q Do you understand --

20 A -- they're common allegations.

21 Q Do you understand that not being truthful
22 under oath today is a felony?

23 A Yes, sir.

24 Q Okay.

25 MR. MILLER: Object. This is --

1 Q The testing that you did with the ES&S BMD
2 years ago, was that cybersecurity testing?

3 A No, it was accessibility testing.

4 Q You've never done cybersecurity testing on
5 BMD equipment or software; is that right?

6 A I don't -- what do you mean by "cyber"?

7 So I just -- as I explained, I created a
8 transparent voting machine which we did election
9 security testing to get at a vulnerability
10 Dr. Halderman had identified as voters not
11 verifying. So that's an example where I have done a
12 test of election security, not cybersecurity.
13 Election security.

14 Q Thank you. That's a fair distinction.
15 Let me ask a better question.

16 As I understand it, you have not conducted
17 any test to determine the extent to which any BMD
18 software or hardware can be hacked; is that fair?

19 A Can be hacked? I have not hacked any,
20 so -- that's not what I do. I don't know if that
21 answers your question or not. But I don't hack
22 these systems. I said that time and time again.

23 MR. MILLER: David, I don't know where you
24 are on your timeline. Do you want to take a short
25 break and come back, if that's all right with you?

1 BY MR. CROSS:

2 Q As you sit here today, do you have any
3 reason to believe that Georgia is auditing anything
4 other than a single election statewide every two
5 years?

6 A I don't -- I don't know.

7 Q So for any election where Georgia is not
8 conducting an RLA, do you understand that the QR
9 code is the only thing that gets tabulated?

10 A In any election that they don't do an RLA,
11 then the QR code would be the tabulation that comes
12 from a computer that is a scanner. I'm going to
13 refer to it as a scanner.

14 Q And you understand for any election where
15 there's no RLA but there's a recount, the recount
16 relies on the QR code. They just run the ballots
17 back through the scanners.

18 Do you understand that, sir?

19 A No, I do not.

20 My understanding, I believe -- again, I
21 have to go back to those previous declarations where
22 I -- my understanding is that they would actually
23 recount the human-readable text.

24 Q Even in a recount as opposed to a
25 risk-limiting audit?

1 A Find what change?

2 Q That their ballot, even as to the
3 human-readable text, does not accurately reflect all
4 of their selections.

5 A Those studies suggest that a few number
6 would identify a human-readable change on that
7 ballot.

8 Q In the scenario where that happened, where
9 both the QR code and the human-readable text has
10 been changed with respect to one or more selections
11 voters made, an RLA would not detect that; right,
12 sir?

13 A If a human didn't detect the change, then
14 the RLA would not detect it if the QR code and the
15 human-readable text match.

16 Q In the State of Georgia, even if an RLA
17 were to find -- strike that.

18 In the State of Georgia, even if an RLA
19 were to generate a different outcome for an election
20 than what was originally reported and certified
21 based on the tabulation of running the ballots
22 through the scanners at the polls, there's no legal
23 authority in Georgia that allows the Secretary of
24 State or anyone to rerun the election, right?

25 MR. MILLER: Objection. Calls for a legal

1 know -- I haven't seen any data to see how accurate
2 it is, how it works. I haven't seen any of that.

3 Q That's not something you considered for
4 your opinions; is that right?

5 A I haven't seen it, so I don't know that I
6 can opine on that as far as Dominion's -- how they
7 do it, the accuracy. I don't have any knowledge of
8 that.

9 Q Do you share Dr. Shamos's recommendation
10 against using QR codes with BMDs for elections in
11 the United States?

12 A I think BMDs can -- QR codes can be used,
13 so I'm not totally against them. But I think -- if
14 I had my choice, I would recommend not using them to
15 eliminate all these discussions and concerns around
16 them.

17 Q Looking at paragraph 15 of your July
18 declaration again -- and if you need to pull that up
19 again, Dr. Gilbert, feel free. It's --

20 A I got it.

21 Q Okay.

22 A Okay. I got it. Yeah.

23 Q Where you indicate here that you're not
24 aware that Dr. Halderman has provided equipment
25 marred by undetectable hacks to any other

1 Q Are you aware that no one at the Secretary
2 of State's office has actually reviewed
3 Dr. Halderman's report?

4 A No, I'm not aware of that.

5 Q Does that surprise you?

6 A I don't have an opinion either way. I
7 don't know.

8 Q Given the many findings Dr. Halderman has
9 about the security of the election equipment used in
10 Georgia, wouldn't you expect those who are
11 responsible for administering elections to at least
12 read the report to determine whether they need to
13 address any of those findings?

14 MR. MILLER: Objection. Asked and
15 answered.

16 THE WITNESS: I don't -- I don't have an
17 opinion. I think someone should read it. I don't
18 know who. I don't know the protocols of chain of
19 custody and how those things work in the State of
20 Georgia, so I can't answer that directly because I
21 don't -- these are things that I don't know and are
22 outside of my expertise.

23 BY MR. CROSS:

24 Q We talked about the Michigan and Rice
25 voter verification studies, and one thing you

1 pointed out about those was that they did not occur
2 in a real election, right?

3 A Right.

4 Q And then we talked about the Georgia voter
5 verification study that the Secretary of State
6 commissioned. One of the things you pointed out
7 about that is they didn't flip votes like they did
8 in the Michigan and Rice studies, right?

9 A I haven't read it, but I suspect they
10 didn't flip the votes.

11 Q Is it your opinion that the only way to
12 conduct a valid study of voter verification is to do
13 it in an actual election where you're flipping
14 votes?

15 MR. MILLER: Objection to form.

16 THE WITNESS: No.

17 BY MR. CROSS:

18 Q So you're not suggesting that that's
19 required, right?

20 A No, I am not.

21 Q And the study that you've talked about
22 today that you performed with your new BMD prototype
23 has the same condition as the Michigan and Rice
24 studies in that that was not conducted in a real
25 election, right?

1 A Correct.

2 Q Are you aware that you're the only expert
3 in this case retained by defendants that, to our
4 knowledge, has even read Dr. Halderman's July 1
5 report?

6 A I was not aware.

7 Q Does that concern you?

8 A You just informed me. I haven't had a
9 chance to form an opinion on it. I don't know. I'd
10 have to think about it.

11 Q As you sit here today as an election
12 security expert, does that raise any concern for
13 you?

14 A I don't know. I'd like to hear more
15 context around why that is. It generates questions
16 for me, and I don't know. I don't have an opinion
17 at this point. It's something I have to digest and
18 then think about.

19 Q What questions does it generate?

20 A First of all, why is that the case? Is
21 there -- there may be a justification for that. I
22 don't know.

23 Q What justification comes to mind?

24 A I don't have one.

25 MR. MILLER: Objection. Relevance.

1 counties could find themselves conducting all sorts
2 of investigations every time somebody makes a claim,
3 right?

4 MR. MILLER: Objection. Calls for
5 speculation.

6 THE WITNESS: I have some work that I'm
7 doing in that area which is confidential at the time
8 that I'm not privy to talk about, unfortunately.

9 But to kind of help with that question,
10 that is something that needs to be addressed. I
11 don't -- I don't know what the protocols are in
12 Georgia or any place where, you know, these things
13 happen with paper ballots. They just spoil it, and
14 you do it over. And that's -- that's essentially
15 what happens if there's a mistake found.

16 But, like, in Florida in 2018 when all
17 those undervotes happened, and South Florida,
18 Broward County, some people spoiled their ballots or
19 had an issue, and they were able to get it right.
20 But no one thought that, "Wait a minute, we have a
21 problem here."

22 So it can happen on both sides.

23 BY MR. CROSS:

24 Q I think you testified a moment ago that
25 with DREs, there would be no way to determine

1 whether a vote was flipped because there's no paper
2 trail. But that's true of BMDs as well, right?

3 If a voter comes and says, "Hey, this
4 ballot flipped my vote," the poll worker has no
5 ability to determine whether that's accurate looking
6 at the ballot or looking at the BMD, right?

7 A In the current state, meaning the current
8 state of BMDs, if that was to happen, the poll
9 worker could not determine if it was a mistake on
10 the voter's part or the -- an error or anything like
11 that. I don't know how they would determine it by
12 just looking at the paper itself.

13 MR. MILLER: David, I'm not sure where you
14 are on your outline, but at an appropriate time, I
15 think a short lunch break might be good.

16 MR. CROSS: Sure. We're almost at a
17 breaking point.

18 Q Do you mind just a few more minutes,
19 Dr. Gilbert?

20 A I'm fine.

21 Q Okay. So take as an assumption based on
22 what I was able to look up that approximately
23 5 million voters voted in the presidential election
24 in Georgia in 2020. Okay?

25 A Okay.

1 But yeah, I think that what I'm getting
2 at, the point that I'm making is a small number of
3 individuals whose votes get flipped would speak up,
4 and this would -- I don't know what the protocols
5 are or the steps are. Again, that's something we're
6 working on, what to do when this occurs. But I
7 don't know what the scenarios are currently in place
8 for something like this.

9 MR. CROSS: Let's go off the record.

10 THE VIDEO OPERATOR: Okay. Going off the
11 record at 1:08.

12 (Recess, 1:08 p.m. - 1:45 p.m.)

13 THE VIDEO OPERATOR: Back on the record at
14 1:45.

15 BY MR. CROSS:

16 Q Dr. Gilbert, we've talked about a couple
17 of ways that you've identified where hand-marked
18 paper ballots can be altered such as with changing
19 undervotes and overvotes, right? We talked about
20 that today?

21 A Right.

22 Q That can only happen after the ballots
23 have been tabulated in a system where the ballots
24 are tabulated on the scanner in the polls, right?

25 A It happens whenever the opportunity

1 presents itself. So it depends on the precinct and
2 how they handle their ballots. If they -- do the
3 voters automatically do it? Is it a centralized
4 tally? It just depends on the scenario.

5 Q So let's talk about a specific scenario, a
6 scenario in which Georgia has voters vote on
7 hand-marked paper ballots at the polls. That voter
8 takes that ballot, walks over to the scanner in
9 exactly the way they do today, and puts it into the
10 scanner themselves.

11 The only way that that vote could be
12 altered or that ballot could be altered in the way
13 that you've described would be after it runs through
14 the scanner and is tabulated, right?

15 A In that particular scenario, that seems to
16 be the case.

17 Q And so whatever alteration might happen to
18 that ballot after it's tabulated would not affect
19 the outcome of that election based on the results
20 that come out of the tabulation of the ballots,
21 right?

22 A Not necessarily.

23 My understanding is that certain margins
24 require an audit or recount; therefore, it would
25 have an impact.

1 background, so I cannot speak to his credentials.

2 The fact that he was appointed to some
3 commission and given a title does not guarantee he
4 knows what he's doing or his credentials. So I
5 can't speak to that. I'm sorry.

6 BY MR. CROSS:

7 Q No, no. That's fair. That's fair.

8 You're not disputing that experts like
9 Dr. Halderman and Dr. Appel have the necessary
10 computer science expertise to evaluate the security
11 of election systems like that used in Georgia,
12 right?

13 A No, I do not dispute that. In fact, if I
14 was asked the question, "I have an election system.
15 We need someone to evaluate the security of it to
16 find vulnerabilities," at the top of my list would
17 be Appel, Halderman. That's where I would start.

18 Q Now, if you look here, if you continue on
19 in Exhibit 4, Dr. Lee goes on to say, "I ultimately
20 chose to vote against the Commission's final report
21 even though we agreed on many points."

22 Do you see that?

23 A Yes.

24 Q If you go to the next paragraph, he
25 writes, "The SAFE Commission was charged with

1 top.

2 A I got it. I got it. I'm on that page
3 now.

4 Q Okay. If you come down below, do you see
5 the third paragraph where Dr. Halderman wrote, "To
6 assist the Court in understanding the risks that the
7 system creates, Curling Plaintiffs asked me to
8 conduct a security analysis of the ImageCase X (ICX)
9 BMD and associated equipment used in Georgia
10 elections"?

11 Do you see that?

12 A I do see that.

13 Q Were you asked, for the purpose of your
14 engagement, to conduct the same type of analysis or
15 were you asked to do something different?

16 A I was not asked to do that. No, I was
17 not.

18 Q If you come down below, you'll see the
19 next heading is "Principal Findings."

20 Do you see that?

21 A Yes, I do.

22 Q And then at the bottom, you'll see, just
23 before the number 1 paragraph, it reads, "The most
24 serious vulnerabilities I discovered include the
25 following."

1 Do you see that?

2 A I do.

3 Q And in your declaration, you don't dispute
4 that any of the number of vulnerabilities that he
5 has in paragraphs 1 through 7 are present in the
6 election equipment used in Georgia, right?

7 MR. MILLER: Object to form.

8 THE WITNESS: Number one, alternate QR
9 codes, that -- I trust that he was able to do that,
10 so I don't dispute that.

11 I would say, you know, given access and
12 time that he was given, I think these -- I don't
13 question him being able to accomplish any of these.
14 BY MR. CROSS:

15 Q Come to the -- it's page 7 of 97. Near
16 the top it says, "Mitigation" in bold.

17 A Got it.

18 Q Do you see here -- do you see the
19 sentence, it's the second sentence that begins,
20 "However"?

21 A Yes.

22 Q And Dr. Halderman wrote, "However, merely
23 patching these specific problems is unlikely to make
24 the ICX substantially more secure."

25 Do you see that?

1 A I do.

2 Q In your declaration, you don't disagree
3 with that opinion, right?

4 A I don't agree -- I don't know that I agree
5 or disagree with it as far as what he -- what he's
6 constituting as patching. I don't know what that
7 means. Merely patching, I'm not sure what the
8 context is, what that means.

9 Q You didn't undertake any analysis into
10 what kind of patching could be adopted to mitigate
11 the vulnerabilities he identifies in his report,
12 right?

13 A No, I did not. And I would say that -- I
14 would like -- it would be interesting for
15 Dr. Halderman to say what patching he's referring
16 to.

17 In addition to that, I go back to our
18 previous discussion about this. When he says the
19 patching, is that referencing reliably secure? Is
20 that the same thing or not?

21 Q All right. If you come down, do you see
22 below that, it says, "Main Conclusions"? It's
23 Section 1.2?

24 A Yes, I do.

25 Q And then he's got a number of paragraphs

1 individual voters, which I would also say I would
2 agree with that. Just as I stated earlier, people
3 with disabilities are individual voters, and they
4 want the right to a private ballot and a fair ballot
5 as well. Shouldn't their votes be counted and not
6 be disenfranchised either?

7 So yes, I completely agree with that.
8 Yes. You're right. Individual voters, every one,
9 including those with disabilities.

10 Q I will say, Dr. Gilbert, that we have
11 found something that we're in violent agreement on,
12 particularly for voters with disabilities.

13 A Okay. So he's talking -- the third one is
14 about QR codes. Let's see. In my -- let's see.
15 Let me look for QR codes. Do I talk about QR codes
16 in here?

17 In my declaration, paragraph 12, I talk
18 about QR codes.

19 Q Just so we're clear, you don't dispute
20 that -- strike that.

21 You don't dispute Dr. Halderman's finding
22 that the QR codes and the human-readable text can be
23 altered by hacking the election equipment that's
24 used in Georgia; you don't dispute that, right?

25 A I do not dispute that, given time and

1 access, that you can modify the software or certain
2 malware to change QR codes and the ballot summary.
3 I do not dispute that.

4 Q And you haven't undertaken any analysis to
5 determine how much time it would take for a hacker
6 to do that if they wanted to do it, right?

7 A No, I have not done that. As I mentioned
8 earlier, I don't hack systems. That's not my
9 expertise, so I wouldn't have done that.

10 That's a great question to ask
11 Dr. Halderman, how long does it take to do such an
12 exercise.

13 MR. CROSS: You might want to write that
14 down, Carey.

15 THE WITNESS: And with that, as far as the
16 time it takes, again, that's not my area, but I
17 think it would be interesting to find the answer to
18 that.

19 And I'd be interested -- again, in the
20 same spirit that I mentioned earlier about
21 Dr. Halderman hacking a system and giving it to a
22 third party, the same thing could be true where
23 Dr. Halderman is given a system and then put on the
24 clock to determine how long it takes him to hack it,
25 not one that he's seen for 12 months.

1 A Got it.

2 Q Do you see in the third paragraph down
3 that begins "Fulton County"?

4 A Yes.

5 Q And here Dr. Halderman writes, "Fulton
6 County did not provide the off-the-shelf laser
7 printer used in conjunction with the BMD. Instead,
8 Plaintiffs acquired a unit of the same model, an HP
9 LaserJet M402dne, from a commercial source."

10 Do you see that?

11 A Yes.

12 Q And you don't dispute in your declaration
13 that the printer that's used with the BMD system in
14 Georgia is, in fact, an off-the-shelf printer like
15 the one that Dr. Halderman used, right?

16 A No, I do not dispute that. I don't have
17 access to the actual printer being used, but I
18 didn't dispute that at all.

19 Q And then if you come down, do you see the
20 paragraph that begins, "In July 2021" on the same
21 page, a couple below where we were?

22 A Let's see.

23 Q Two paragraphs --

24 A I got it. I see it.

25 Q Here Dr. Halderman wrote, "In July 2021, I

1 received access to further election system data.
2 State Defendants provided Plaintiffs copies of data
3 sent to the Secretary of State by Georgia counties
4 following the November 2020 and January 2021
5 elections."

6 Do you see that?

7 A Yes.

8 Q He goes on to talk about the election
9 packages that he received.

10 Do you see that?

11 A Yes.

12 Q You don't address that data in your
13 declaration, right?

14 A No, I do not.

15 Q Do I understand, is that not something
16 you've analyzed?

17 A No, I have not analyzed that.

18 Q If you come to the next paragraph, do you
19 see where it reads, "Five of the county data sets"?

20 A Yes.

21 Q He writes, "Five of the county data sets
22 provided by State Defendants contained copies of the
23 installation file for the October 2020 ICX software
24 update, version 5.5.10.32."

25 He goes on to say, "The presence of this

1 file may indicate that the counties returned data to
2 the Secretary on the same USB drives that they used
3 to receive or distribute the software update,
4 without first wiping the device."

5 Do you see that?

6 A Yes.

7 Q And you don't dispute his opinion there on
8 what that indicates in your declaration, right?

9 A I do not discuss that in my declaration.

10 Q You previously testified in this case that
11 your understanding is that the BMD election system
12 is air-gapped, right?

13 A Yes.

14 Q I think you testified before that you're
15 assuming that to be true based on some materials you
16 looked at describing how the system is supposed to
17 operate and be set up; is that right?

18 A Correct.

19 Q You've not yourself confirmed that any
20 aspect of Georgia's election system is, in fact,
21 air-gapped, right?

22 A I have not had a Georgia system in my
23 possession to do any evaluation.

24 Q And you did not undertake any analysis or
25 investigation with your client in this case to

1 determine whether the election system is in any way
2 air-gapped, right?

3 A No. I use -- I cited in my previous
4 declarations what I used. Those documents were
5 referenced in my declaration.

6 Q You did not undertake any analysis or
7 investigation to determine whether any equipment or
8 devices that were used with the old DRE system have
9 also been used with the new BMD system, right?

10 A All I had was what I put in my
11 declaration, the documents that I referenced. I
12 didn't have access to an old DRE, I did not have
13 access to the new BMD or any election system. I
14 have not had access to any election system from the
15 State of Georgia ever.

16 MR. CROSS: Oh, why did it do that? Hold
17 on. Sorry. I was just pulling up a new exhibit.
18 It's going to be Exhibit 6. Give me one second.

19 (Exhibit 6 was marked for identification
20 and is attached hereto.)

21 BY MR. CROSS:

22 Q All right. Pull up Exhibit 6, if you
23 would, please, Dr. Gilbert. Just let me know when
24 you have it.

25 Hold on. Sorry. It's Exhibit -- it's

1 Q Are you aware that this is an exhibit that
2 we introduced during the hearing in September of
3 last year in which you also testified?

4 A Like I said, I don't remember this, but
5 okay.

6 Q There's no indication in your declaration
7 that you've had any -- conducted any investigation
8 into what's being discussed here and whether USB
9 drives that were used with the DRE system have also
10 been used with the new BMD system. That's not
11 something you've looked into, correct?

12 MR. MILLER: Objection. Relevance.

13 THE WITNESS: No, I have not.

14 BY MR. CROSS:

15 Q And you previously testified in this case
16 that the new BMD system is completely separate and
17 unconnected to the old DRE system, right?

18 A Yes, I did.

19 Q But if the counties were using USB drives
20 with the new Dominion system that they previously
21 had used with the DRE system, that certainly would
22 raise the possibility for an exchange of data
23 between those two systems, right?

24 MR. MILLER: Objection. Relevance.

25 THE WITNESS: I think you said it

1 correctly. Possibility.

2 So it's possible that these drives could
3 have been completely wiped and reformatted. It's
4 possible that they could have been tainted. So it's
5 possible a lot of different things based on what you
6 are saying.

7 BY MR. CROSS:

8 Q You didn't think that it was relevant for
9 your opinions in this case to determine whether the
10 counties or the state are using USB drives with the
11 new system that were previously used with the DRE
12 system without wiping them, without securing them,
13 without ensuring that they're not compromised?

14 A I did not ask that question.

15 Q Do you think that that's a relevant
16 question for evaluating the security of the new
17 election system?

18 A I think that is a relevant question, and
19 it should be asked.

20 I think the protocol of what's obviously
21 exchanged -- anything connected to the voting system
22 should be evaluated, obviously.

23 Q Evaluated how?

24 A All kinds of ways. It depends on what
25 you're connecting to it.

1 Q I'm sorry. Can you explain what you mean?

2 A For example, if you're connecting a USB to
3 the system, it should be wiped. That's a clean -- a
4 way to clean the -- keep the system clean, avoid
5 issues. Standard protocol in many places in shops
6 that have technology.

7 So evaluating what is connected, what's
8 the data on there, those questions are things that
9 have to be looked at.

10 Q Why didn't you look at that on behalf of
11 the state with respect to things like the USB drives
12 that we see being discussed here for your work?

13 A I was -- I was focused on what was
14 given -- I was not given USB drives. I was not
15 given any technology.

16 My focus, again, was on Dr. Halderman and
17 Appel's analysis. That's where my focus was on. I
18 don't have any equipment, never have received any
19 equipment, technology, from the State of Georgia.

20 Q If you come back to Dr. Halderman's
21 report, the July 1 report, the page we were on
22 before, page 19 of 97 --

23 A Okay.

24 Q -- at the bottom, do you see where it
25 says, Section 4.3, "Testing Process"?

1 A Yes, I do.

2 Q You don't offer an opinion in this case
3 that Dr. Halderman's methodology for his analysis in
4 his report was in any way improper or unsound,
5 right?

6 A I do not.

7 Q Come to page 22 of 97. You'll see there's
8 a heading in the middle of the page, Section 5.2,
9 "Defeating QR Code Authentication."

10 A Yes.

11 Q And here he writes, "Issue: ICX QR codes
12 are not protected against 'replay' attacks, so
13 copies of valid QR codes will be accepted as
14 genuine."

15 Do you see that?

16 A Yes.

17 Q You don't dispute in your declaration that
18 ICX QR codes are not protected against replay
19 attacks, right?

20 A I do not.

21 Q If you come down to page 24 of 97, do you
22 see where it says, "Copying Ballots"?

23 A Yes.

24 Q And here he wrote, "A copy of a genuine
25 ICX ballot will be indistinguishable from a second

1 genuine ICX ballot with the same votes. In tests,
2 the ICP accepted ballots copied using an office
3 photocopier," and he refers to Section 11.1. He
4 says, "This could allow a variety of ballot-box
5 stuffing attacks."

6 Do you see that?

7 A I do see that.

8 Q And you don't dispute in your declaration
9 his finding on the ability to copy the ballots,
10 right?

11 A I do not.

12 Q Next, he refers again to the replay
13 attack.

14 Do you see that?

15 A Yes.

16 Q Come to page 29 of 97.

17 A Okay.

18 Q Do you see there's a picture at the top
19 of -- it looks like access cards?

20 A Yep.

21 Q Do you see where it says, "Forged ICX
22 Smart Cards"?

23 A Yes.

24 Q And then he writes, "Weaknesses in the ICX
25 authentication protocol allow an attacker to read

1 and forge Voter, Technician, and Poll Worker cards."

2 Do you see that?

3 A Yes, I do.

4 Q He goes on to say at the end, "a real
5 attacker could go on to create nearly
6 indistinguishable counterfeits."

7 Do you see that?

8 A I do.

9 Q You don't dispute that finding in your
10 declaration, right?

11 A I do not.

12 Q If you come down to the heading 6.1 on the
13 same page --

14 A Yep.

15 Q -- it reads, "Extracting Election Secrets
16 from Poll Worker Cards."

17 Do you see that?

18 A I do.

19 Q Here he writes, "Anyone with access to a
20 single Poll Worker Card and the corresponding PIN
21 can easily extract secret keys and other values used
22 for securing election data throughout the county."

23 Do you see that?

24 A I do.

25 Q And you don't dispute that finding in your

1 declaration, right?

2 A I do not.

3 Q All right. Come to the next page, heading
4 6.2.

5 A Yes.

6 Q It says, "Forging Technician Cards to
7 Install Malware on any ICX."

8 Do you see that?

9 A I do.

10 Q And here he writes, "Anyone can create
11 forged Technician Cards without using any secret
12 information. Such cards can be used to access any
13 ICX's Android operating system and the ability to
14 install malware."

15 Do you see that?

16 A I do.

17 Q And you don't dispute that finding in your
18 declaration, right?

19 A No, I do not.

20 Q Come down to the next page, please,
21 heading 6.3.

22 A Got it.

23 Q Here it reads, "Creating 'Infinite' Voter
24 Cards."

25 Do you see that?

1 A Yes.

2 Q He writes, "Voters can clone Voter Cards
3 or create 'infinite' Voter Cards that allow printing
4 an unlimited number of ballots of any available
5 ballot style."

6 Do you see that?

7 A I do.

8 Q You don't dispute that finding in your
9 declaration, correct?

10 A I do not.

11 Q Come to the next page, 33 of 97,
12 heading 7.

13 A Page 33, you said?

14 Q Yes, sir. Heading 7.

15 A I'm there.

16 Q Okay. Come down to heading 7.1.

17 Do you see that?

18 A Yeah, I'm there.

19 Q He writes, "The ICX does not require that
20 applications be signed by a trusted source, allowing
21 the installation of arbitrary APKs."

22 Do you see that?

23 A Yes.

24 Q You don't dispute that finding in your
25 declaration, correct?

1 A I do not.

2 Q Come to the next page, please,
3 heading 7.2.

4 A Yes.

5 Q Here he writes -- the heading is
6 "Obtaining the Real APK." And he writes, "The ICX
7 App's APK can be easily extracted given only brief,
8 one-time access to a single BMD."

9 Do you see that?

10 A Yes.

11 Q You don't dispute that finding in your
12 declaration, correct?

13 A I do not.

14 Q Go on page 36 of 97, please.

15 A Okay.

16 Q He has heading 7.5, "Defeating Applicable
17 Defenses."

18 Do you see that?

19 A I do.

20 Q He writes, "Malware running on the ICX can
21 defeat the various technical and procedural defenses
22 that the Dominion system in the State of Georgia
23 currently employ."

24 Do you see that?

25 A I do.

1 Q You don't dispute that finding in your
2 declaration, correct?

3 A I don't think I dispute this. No, I do
4 not.

5 Q And then he goes on to refer to defeating
6 logic and accuracy testing.

7 Do you see that?

8 A I do.

9 Q And he -- at the end of that paragraph, he
10 concludes, "It can be easily defeated by ICX
11 malware."

12 Do you see that?

13 A At the end of that paragraph? I don't see
14 it.

15 Q Do you see the short paragraph that has
16 the bolded language, "Defeating Logic and Accuracy
17 Testing"?

18 A Yeah, I do.

19 Q If you come to the end of that short
20 paragraph, the last sentence reads, "It can be
21 easily defeated by ICX malware."

22 A I don't see that anywhere. I see
23 "Defeating the QR code" --

24 Q You're too far down. I'm sorry. Come up
25 above -- just below the heading 7.5, the bolded

1 language, "Defeating Logic and Accuracy Testing."

2 A Okay. I'm there.

3 Q So stay in that same short paragraph.

4 A I see it. I see it. "It can be easily
5 defeated by ICX malware." I see it now. The last
6 sentence in that paragraph. Okay.

7 Q Yes. And you don't dispute that finding
8 in your declaration, right?

9 A I did not dispute that in my declaration.

10 Q Okay. If you come down to where you were
11 looking at a moment ago, the bolded language at the
12 bottom of that page that reads, "Defeating the QR
13 Code MAC," do you see that?

14 A Yes.

15 Q At the end of that paragraph, still on the
16 same page, he concludes, "This poses no obstacle to
17 ICX malware."

18 Do you see that?

19 A Yes.

20 Q You did not dispute that finding in your
21 declaration, correct?

22 A No, I did not.

23 Q Okay. Come to the next page, please.

24 A Okay.

25 Q Do you see at the bottom of the next page

1 there's a bold heading, "Defeating APK Hash
2 Validation"?

3 A Yes.

4 Q If you come down just three or four lines,
5 the sentence that begins "However"?

6 A Yes.

7 Q He writes, "Much like the QR code MAC,
8 this hash value is computed by the ICX App itself
9 and can therefore be trivially defeated by malicious
10 logic added to the app."

11 Do you see that?

12 A Yes.

13 Q You don't dispute that finding in your
14 declaration, right?

15 A I did not.

16 Q If you come to the next page --

17 A Yes.

18 Q -- at the top he writes, "Defeating
19 External APK Validation."

20 Do you see that?

21 A Yes.

22 Q Come to the beginning of the very next
23 paragraph. Do you see where it begins, "A malicious
24 ICX App"?

25 A Yes.

1 Q And he writes, "A malicious ICX App can
2 easily defeat this safeguard, too, because the
3 export process is performed by the app itself."

4 Do you see that?

5 A I do.

6 Q You don't dispute that finding in your
7 declaration, right?

8 A I do not.

9 Q Come to the next bold heading on the same
10 page that reads, "Defeating Voter Verification and
11 Auditing."

12 Do you see that?

13 A Yes.

14 Q He writes, "Voters have no practical way
15 to verify the contents of QR code," right?

16 A Right.

17 Q And we're agreed on that, right?

18 A Yes. To my knowledge, I don't know how
19 they would verify it. The only way I've seen
20 that -- and I don't -- I haven't seen this. But I
21 know other systems -- and when we designed -- we
22 designed this many years ago -- take the ballot and
23 stick it in another machine to get a summary
24 display, or have the tally, the scanner, give you
25 a -- I guess a ballot summary, and you can compare

1 it to the ballot summary that's on there.

2 But I -- other than that, people cannot
3 read the QR code itself.

4 Q One of the things you suggested in an
5 earlier declaration in this case is that the state
6 should do parallel testing of a single BMD during an
7 election.

8 Do you recall suggesting that?

9 A Yes.

10 Q Do you think that testing a single BMD out
11 of over 30,000 that are used across the state
12 provides a meaningful test of the security and
13 reliability of those BMDs as a whole?

14 A That's not what I recommended. But to
15 answer your question, no, that would not. You have
16 all those, and you're just testing one? No, that
17 wouldn't make a difference. But if you test one in
18 every precinct, that's different.

19 Q Okay. So it's your recommendation to test
20 one in every precinct during the election in
21 parallel testing?

22 A That is something I have recommended. It
23 has pros and cons. But that's way better than just
24 picking one particular BMD in the State of Georgia
25 and parallel testing it. Yeah, that wouldn't make

1 much sense.

2 Q Okay. Come to page 40 of 97 in
3 Dr. Halderman's report, section heading 8.1.

4 A Got it.

5 Q You see it reads, "Attaching USB Devices
6 to the ICX"?

7 A Yes.

8 Q And he writes, "The ICX fails to
9 adequately restrict the kinds of devices that can be
10 attached to its USB ports, including the externally
11 exposed USB cable that connects to the printer."

12 Do you see that?

13 A I do.

14 Q You don't dispute that finding in your
15 declaration, correct?

16 A I do not.

17 Q Come down to the next page under the
18 pictures.

19 A Okay.

20 Q Do you see where it says, "Figure 9"?

21 A Yes.

22 Q And here it reads, "ICX USB Interfaces are
23 Exposed to Voters and Unsealed."

24 Do you see that?

25 A I do.

1 Q Dr. Halderman writes, "A USB cable
2 connects the BMD to an off-the-shelf laser printer.
3 At polling places, the end of the cable attached the
4 to printer is physically accessible to voters, and
5 it is not protected by a tamper-evident seal.
6 Voters could install malware on the ICX by attaching
7 a device to the end of this cable."

8 Do you see that?

9 A I do.

10 Q And you don't dispute that finding in your
11 declaration, correct?

12 A I do not.

13 Q Come to the top of the next page, please.

14 A Okay.

15 Q You see there's a picture, and below that
16 it says, "Figure 10"?

17 A Yes.

18 Q And then it reads, "Attaching a USB Device
19 to the ICX via the Printer Cable."

20 Do you see that?

21 A I do.

22 Q And here Dr. Halderman writes, "The BMD's
23 USB cable is not sealed to the printer, and voters
24 can simply reach behind the printer and disconnect
25 it. Using an inexpensive and widely available

1 adapter, any standard USB device (such as the
2 keyboard shown)" -- in the pictures -- "can attach
3 to the end of the cable and operate as if it were
4 plugged in directly to the ICX."

5 Do you see that?

6 A I do.

7 Q And you do not dispute that finding in
8 your declaration, correct?

9 A I do not.

10 Q Go to section heading 8.2.

11 A Okay.

12 Q It reads escaping the ICX app.

13 Are you with me?

14 A Yes, I am.

15 Q And then Dr. Halderman writes, "As a
16 result of Georgia's installation of a software
17 update in October 2020, the ICX's Android operating
18 system settings can be accessed by attaching a USB
19 keyboard, allowing the installation of malware."

20 Do you see that?

21 A I do.

22 Q And you don't dispute that finding in your
23 declaration, right?

24 A I do not.

25 Q If you stay in that same section, do you

1 see the very next paragraph begins, "In
2 October 2020"?

3 A Yes, I see it.

4 Q Dr. Halderman writes, "In October 2020,
5 shortly before the start of early voting in the
6 November election, Georgia installed a purportedly
7 de minimis software update on its BMDs to correct a
8 user-interface glitch."

9 Do you see that?

10 A Yes.

11 Q In the next paragraph he writes, "My
12 testing shows that installing the ICX software
13 update did indeed create a dangerous security
14 problem. It left the BMDs in a state where anyone
15 with physical access, including non-technical
16 voters, could install malicious software."

17 Do you see that?

18 A I see that.

19 Q You don't dispute that finding in your
20 declaration, correct?

21 A I do not.

22 Q If you stay on that same page, the
23 paragraph we just read, do you still have that in
24 front of you?

25 A I do.

1 Do you see that?

2 A I do.

3 Q And then Dr. Halderman writes, "The ICX
4 has built-in Terminal Emulator app that is
5 configured so that the user can easily obtain a
6 command-line shell with supervisory privileges."

7 Do you see that?

8 A Yes.

9 Q You don't dispute that finding in your
10 declaration, correct?

11 A I do not.

12 Q All right. Come to the next page, please,
13 under heading 8.5.

14 A Okay.

15 Q And here it reads, "Automating Malware
16 Installation," right?

17 A Yes.

18 Q And Dr. Halderman writes, "The process
19 described above can be completed" -- I'm sorry. Let
20 me try that again.

21 Here Dr. Halderman writes, "The process
22 described above can be completely automated, so that
23 an attacker can install malware by attaching a
24 single USB device to the exposed printer cable for
25 less than two minutes. The automated process is

1 simple and fast enough that it could potentially be
2 carried out by a voter in the polling place."

3 Do you see that?

4 A Yes.

5 Q And you don't dispute that finding in your
6 declaration, correct?

7 A I do not.

8 Q Come to page 47 of 97, please.

9 A Okay.

10 Q Actually, go up one page -- sorry -- to
11 page 45 of 97 just so you see the heading 8.6 at the
12 bottom.

13 A Got it.

14 Q It reads, "Local Malware Installation
15 using a Forged Technician Card."

16 Do you see that?

17 A I do.

18 Q If you come to the top of the next page,
19 do you see at the very top of that page
20 Dr. Halderman writes, "One is to use a forged
21 Technician Card created using the technique
22 described in Section 6.2, which requires no secret
23 passwords, keys, or PINs, but only a widely
24 available \$10 Java Card with some simple
25 programming."

1 Do you see that?

2 A I do.

3 Q You don't dispute that finding in your
4 declaration, correct?

5 A I do not.

6 Q All right. Come down to the next section,
7 please, 8.7.

8 A Okay.

9 Q Here it reads, "Local Malware Installation
10 via Android Safe Mode."

11 Are you with me?

12 A Yes.

13 Q Here Dr. Halderman writes, "A local user
14 can reboot the ICX into 'Safe Mode,' allowing full
15 control of the Android operating system."

16 Do you see that?

17 A Yes.

18 Q You don't dispute that finding in your
19 declaration, correct?

20 A I do not.

21 Q Come to page 50 of 97, please.

22 A Okay.

23 Q Do you see at the top there's what looks
24 to be some computer code and then it says, "Issue"
25 underneath?

1 A Yep.

2 Q And here Dr. Halderman writes, "ICX
3 election definition files are not digitally signed,
4 and they can be modified by anyone with access to a
5 symmetric encryption key that is shared by all
6 scanners and BMDs within each county."

7 Do you see that?

8 A I do.

9 Q You do not dispute that finding in your
10 declaration, correct?

11 A I do not.

12 Q Then if you come down one paragraph, do
13 you see the heading that reads "Distribution and
14 Points of Attack"?

15 A I do.

16 Q If you come down to the second paragraph
17 under that heading, do you see where it reads --
18 it's just two sentences -- two lines -- it reads,
19 "This election definition"?

20 A I do.

21 Q In there Dr. Halderman writes, "This
22 election definition distribution process introduces
23 two kinds of opportunities for remote malware
24 attacks," and he identifies two examples, one at the
25 county level, one at Dominion.

1 Do you see that?

2 A I do.

3 Q You don't dispute that finding in your
4 declaration, correct?

5 A I do not.

6 Q Come to the next -- top of the next page,
7 please.

8 A Okay.

9 Q Do you see section 9.2, "Directory
10 Traversal Vulnerability"?

11 A I do.

12 Q Here Dr. Halderman writes, "The ICX
13 software contains a critical directory traversal
14 vulnerability that allows a maliciously modified
15 election definition file to overwrite arbitrary
16 files."

17 Do you see that?

18 A I do.

19 Q You don't dispute that finding in your
20 declaration, correct?

21 A I do not.

22 Q Come down to the next section, please,
23 9.3.

24 A Okay.

25 Q It reads, "Arbitrary Code Execution as

1 Root."

2 Do you see that?

3 A I do.

4 Q Here Dr. Halderman writes, "The BMD runs
5 code with root privileges from a file that is
6 writable by the ICX App. When combined with the
7 directory-traversal vulnerability, this allows a
8 malicious election definition file to execute
9 arbitrary code as root."

10 Do you see that?

11 A I do.

12 Q You do not dispute that finding in your
13 declaration, correct?

14 A I do not.

15 Q Come to page 54 of 97, please.

16 A I'm there.

17 Q Do you see the heading 9.6, "Conclusions"?

18 A I do.

19 Q Do you see the second paragraph that
20 begins, "Security experts"?

21 A Yes.

22 Q Here Dr. Halderman writes, "Security
23 experts consider arbitrary code execution to be one
24 of the most dangerous classes of vulnerabilities,
25 particularly when it can be exploited to run code

1 with root privileges, as it can on the ICX."

2 Do you see that?

3 A I see it.

4 Q You don't disagree with that statement in
5 your declaration, correct?

6 A I do not.

7 Q You see he goes on to explain --
8 Dr. Halderman does -- "In 2006, Harri Hursti
9 discovered a similar arbitrary code execution
10 vulnerability that affected Georgia's old AccuVote
11 TS-X DREs."

12 Do you see that?

13 A Yes.

14 Q Do you recall that vulnerability that was
15 discovered?

16 A I do not.

17 Q Dr. Halderman explains, "At the time,
18 Defendants' expert Michael Shamos called it 'the
19 most serious security breach that's ever been
20 discovered in a voting system.'"

21 Dr. Halderman concludes, "The
22 vulnerabilities in the ICX are as or more severe."

23 Do you see that?

24 A I see it.

25 Q And you don't dispute that finding in your

1 declaration that the vulnerabilities in the ICX are
2 as or more severe, right?

3 A I do not dispute it in my declaration, but
4 I do not agree with it.

5 Q And what's the basis for disagreeing with
6 that when you've not examined the security -- the
7 cybersecurity of the equipment at issue here?

8 A I don't need to examine it to make this
9 statement.

10 The DRE does not have a paper trail. If
11 there's a vulnerability on the BMD and voters verify
12 it, you can catch it. In other words, you can
13 prevent it. He can hack it and change it all he
14 wants. But if they are verifying it, he can't
15 change the outcome of the election. He can't
16 disenfranchise people. The DRE, you can change it
17 and it's impossible to know.

18 So Dr. Shamos is right in the context of
19 the DRE, but that doesn't apply to a BMD the same
20 way. It is not the same.

21 Q Voter verification does not prevent any of
22 the hacks that Dr. Halderman has identified from
23 occurring, right?

24 A Voter verification would not prevent the
25 hack from occurring. It would prevent the hack from

1 needed to protect the voter, which is there also has
2 to be an audit, right? A reliable audit?

3 A It depends on the -- on the technology and
4 how it all fits together.

5 But we recommended for the NASEM report
6 that if you're going to have a scanner, then you
7 need to have an audit because the scanner could be
8 compromised.

9 Q All right. I'm sorry. Take a look at
10 page 55 of 97 now, heading 10.1.

11 A Got it.

12 Q Here you have the heading "Vulnerable
13 Storage Design."

14 Do you see that?

15 A I do.

16 Q And Dr. Halderman writes, "ICX audits logs
17 and protective counters are stored in regular files
18 with no protection beyond filesystem permissions,
19 which can be easily bypassed."

20 Do you see that?

21 A Yes.

22 Q You don't dispute that finding in your
23 declaration, correct?

24 A I do not.

25 Q He then goes on in the same section, "The

1 ICX does not provide any mechanism to verify the
2 integrity of exported audit logs."

3 Do you see that?

4 A I do.

5 Q You don't dispute that finding in your
6 declaration, correct?

7 A I do not.

8 Q Come to the page 57 of 97, please.

9 A I'm there.

10 Q Do you see the heading 11.1, "The ICP
11 Accepts Photocopied Ballots"?

12 A Yes.

13 Q Here Dr. Halderman writes, "The ICP as
14 tested did not require ballots to be printed on
15 security paper, and it accepted ICX ballots
16 photocopied on normal office paper."

17 Do you see that?

18 A I do.

19 Q You did not dispute that finding in your
20 declaration, correct?

21 A I did not.

22 Q Do you see the next heading, 11.2, on the
23 same page?

24 A I do.

25 Q Here it reads, "A Dishonest Poll Worker

1 with Access to the ICP Memory Card can Deanonymize
2 All Voted Ballots."

3 Do you see that?

4 A I see it.

5 Q Dr. Halderman writes, "The ICP tested does
6 not encrypt ballot images stored on its memory
7 card."

8 Do you see that?

9 A I do.

10 Q You do not dispute that finding in your
11 declaration, correct?

12 A I do not.

13 Q Dr. Halderman goes on here to write, "ICP
14 memory cards store ballot images in the order they
15 were cast."

16 Do you see that?

17 A I do.

18 Q You do not dispute that finding in your
19 declaration, correct?

20 A I do not.

21 Q Come to the next page, please, Section
22 11.3.

23 A Okay.

24 Q The report itself is not 97 pages long, so
25 we're getting towards the end. I imagine this is

1 getting monotonous.

2 Take a look at Section 11.3. Do you see
3 where it reads, "Installed Tamper-Evident Seal could
4 be Bypassed or Defeated"?

5 A Yes.

6 Q Here Dr. Halderman writes, "The ICP modem
7 port door is incompletely closed when sealed,
8 allowing access to connectors inside."

9 Do you see that?

10 A I do.

11 Q You do not dispute that finding in your
12 declaration, correct?

13 A I do not.

14 Q He then goes on in the same section to
15 write, "The tamper-evident seal on the ICP tested
16 was improperly installed, leaving it easily
17 defeated."

18 Do you see that?

19 A I do.

20 Q You did not dispute that finding in your
21 declaration, correct?

22 A Did not.

23 Q Come to page 62 of 97, please. There's a
24 heading, "References."

25 A Got it.

1 that they made.

2 That doesn't mean that the marks on the
3 ballot are accurate. That doesn't mean that the
4 marks on the ballot will be translated the way they
5 marked it. Their intent is not guaranteed to be
6 captured by the scanner.

7 BY MR. CROSS:

8 Q But if the scanner is operating as it
9 should and they have carefully verified each of the
10 selections on their hand-marked paper ballot, then
11 they can have reasonable confidence that it's going
12 to be tabulated, at the moment it goes into the
13 scanner, correctly, right?

14 MR. MILLER: Object to form.

15 THE WITNESS: It goes back to
16 "reasonable." I don't know to what extent. But
17 hopefully they have complete confidence. Because if
18 they don't, we have an issue with our elections.
19 But there is a level of reasonableness there that's
20 variable.

21 BY MR. CROSS:

22 Q But with a QR code, the voter has no
23 ability -- no matter how carefully they review the
24 ballot, they have no ability to verify that what's
25 going to get tabulated as their vote when it goes

1 into the scanner is accurate even if the scanner is
2 working exactly as it should, right?

3 MR. MILLER: Objection. Asked and
4 answered.

5 THE WITNESS: There's no way for a human
6 being to look at a QR code, to my knowledge, and
7 determine what's in it. So by that definition, you
8 cannot -- you don't know what's in it. You can't
9 read the QR code with your eyes.

10 BY MR. CROSS:

11 Q And that's the same way with the old DREs
12 in Georgia, right? The moment the voter casts their
13 ballot, casts their ballot on the DRE, they have no
14 way to know whether it's going to be counted as they
15 intended because they don't know whether the DRE is
16 working properly, right?

17 MR. MILLER: Objection. Asked and
18 answered.

19 THE WITNESS: The DRE -- there's no way to
20 know if it's even stored, if it's stored as
21 intended, if it's modified. You have no idea of
22 anything.

23 With the QR code, you knew it was
24 successfully scanned. You do have that
25 determination. Just like you do with a hand-marked

1 paper ballot, you know that it was scanned, but you
2 don't know that it read it correctly or even stored
3 it. You don't know that it didn't change your vote.
4 You have no idea what it did in the tally.

5 BY MR. CROSS:

6 Q As an election security expert, do you
7 believe that an election system can be so unsecured
8 that it should not be used?

9 MR. MILLER: Objection.

10 THE WITNESS: Yes.

11 BY MR. CROSS:

12 Q You've prepared something you called a
13 ballot-marking verification protocol, right?

14 A Yes.

15 Q And the conclusion you included in that,
16 you wrote, "Don't trust the BMD. Audit it with the
17 BMVP."

18 Do you recall writing that?

19 A Yes.

20 Q And why did you write that?

21 A Because whenever you use a computing
22 device to do the tally, you cannot trust it. You
23 have to do the audit, which was the conclusion of
24 the National Academies report. That's why we do the
25 audit.

1 If you have hand-marked paper ballots, you
2 have to do the audit because the scanner could lie
3 to you. You can hack the scanner.

4 Q You testified in a case captioned National
5 Federation of the Blind versus Linda Lamone; is that
6 right?

7 A Yes.

8 Q And that was in 2014; is that right?

9 A I don't know the year.

10 Q Do I understand correctly that you
11 testified on behalf of the plaintiffs that were
12 challenging the election system in that case?

13 A No, I don't recall which side I was on. I
14 have to go back and look at my notes. It's been a
15 long time, and I've served on several cases since
16 then.

17 Q You don't recall that you testified on
18 behalf of the National Federation of the Blind?

19 A I do recall that. So were they the
20 plaintiffs?

21 Q Yes.

22 A Whoever they were, that's who I -- what
23 side I was on. Does that help?

24 Q Yes. Yes. Okay. What was the thrust of
25 your opinions in that case on behalf of the National

1 I, the undersigned, a Certified Shorthand
2 Reporter of the State of California, do hereby
3 certify:

4 That the foregoing proceedings were taken
5 before me at the time and place herein set forth;
6 that any witnesses in the foregoing proceedings,
7 prior to testifying, were administered an oath; that
8 a record of the proceedings was made by me using
9 machine shorthand which was thereafter transcribed
10 under my direction; that the foregoing transcript is
11 a true record of the testimony given.

12 Further, that if the foregoing pertains to
13 the original transcript of a deposition in a Federal
14 Case, before completion of the proceedings, review
15 of the transcript [x] was [] was not requested.

16 I further certify I am neither financially
17 interested in the action nor a relative or employee
18 of any attorney or any party to this action.

19 IN WITNESS WHEREOF, I have this date
20 subscribed my name. Dated this 5th day of November, 2021.

21
22
23 Carla Soares

24
25 CARLA SOARES

CSR No. 5908